REMARKS

The examiner objects to the specification as failing to define the term "external agent" as used in claim 10, and the term "communication channel" as used in claim 20 and its descendents. Claims 10, 20, and 28 have accordingly been amended to omit those terms.

The examiner rejects the bulk of the claims by drawing attention to superficial similarities in the structure of the present invention and that of the cited Aggarwal patent, US6873977. In the context of the respective specifications, however, it is quite clear that these inventions not only serve completely orthogonal purposes, but that their structure is not actually similar at all.

As a system for transaction-oriented purchasing, Aggarwal uses packet network signalling and encryption technology in a novel way to provide the advantage of allowing buyers to remain anonymous before sellers. The present invention uses packet network signalling and encryption technology in a different, and also novel, way that provides end to end private messaging with the significant advantage over prior art systems of not requiring end users to have *a priori* knowledge of one another's encryption and authentication certificates. Aggarwal's anonymity goal is not desirable in general messaging, because correspondents do want to know one another's identity; with such clearly opposite system requirements, it is highly unlikely that the two inventions would use identical techniques.

Unlike prior art encrypted messaging systems and also unlike the transaction system in Aggarwal, in the present invention end users are not required to have *a priori* knowledge of one another's encryption and authentication certificates; the trusted couriers handle exchanging these credentials and certifying to one another the validity of their agents, and thereby in turn their users. Where in Aggarwal the goal of using multiple intermediaries is to conceal the buyer's identity from the seller, in the present invention the intermediaries relieve end users and their agent software of the need to exchange certificates with one another. In both inventions, intermediaries present a risk to the end users' privacy, and each one solves this problem in a different manner. Aggarwal uses

multiple encryption within the order message so that any one intermediary cannot decrypt enough of the order to get at its content. The present invention separates the content from the content key and sends them through different elements of the system that do not interact and, if implemented properly, cannot cooperate to combine the message pieces prior to their arrival at the recipient agent. Further, Aggarwal permits the buyer to select a chain of intermediaries explicitly, requiring the user to have exactly the sort of information the present invention conceals from the user as a desirable simplification.

Additional differences beyond these key ones will be described below as they arise in the discussion.

With respect to the rejection of claims 1, 2, 10, and 19, the examiner likens Aggarwal's buyer and seller to the present invention's private messaging agent, and Aggarwal's Aplic1 and Aplic2 to the present invention's foreground and background element. The first of these is a faulty comparison, since the buyer and seller in Aggarwal are clearly humans or autonomous decision-making entities (in other words, users), while the private messaging agent is a tool that acts on behalf of an end user and makes no independent decisions itself. The second comparison indicates a misunderstanding of the two inventions' architectures. Aplic1 and Aplic2 are programs that run at the buyer's client; they are therefore more akin to the present invention's agent than to its foreground and background elements, which reside in trusted couriers. The comparison of Aplic1 and Aplic2 to the private messaging agent is also erroneous, because it is clear from the Aggarwal specification as cited that these two programs are transient - they exist for the duration of a single transaction - while the agent is a persistent object that handles multiple messages over the life of the user's relationship with the courier.

Nevertheless, in order to quell this confusion and draw a clearer distinction between the two inventions, claims 1, 2, 10, and 19 are hereby amended to sharpen their description of the key points in the present invention.

With respect to the rejection of claims 6 and 7, the examiner has missed a fundamental difference between the current invention and the Aggarwal invention. Referring to Figure 2 and its corresponding specification paragraphs, there are several topology options which owners of couriers may choose in constructing trust relationships and message transfer paths with one another, and in selecting the subset of users which they will serve. However, any particular user and agent will associate with exactly one courier, by design, in order to simplify that user's life. Aggarwal intentionally promotes the opposite behavior, so that users (buyers and vendors) have a multitude of banks and coding stations from which to choose in order to increase the desired transaction privacy opportunity. This promotes a randomly meshed topology at every level, very different from the present invention's strict hierarchy for agents with constrained meshing for couriers. In addition, comparison of the present invention with logging on at a home bank, using the citation of US6529885 to Johnson, is inappropriate. A user can bank with multiple banks and thus can access an electronic system by logging onto different banks, whereas in the present invention, a user and agent is associated with exactly one courier. Claims 6 and 7 are amended to clarify this distinction.

With respect to claims 14 and 18, the significant parts of claim 14 (and by reference 18) are novel and reflect key points of the invention: automated handling of encryption/authentication certificates in a way that simplifies life for and hides details from the messaging end user, and routing of message content separate from the content key. Claim 14 is hereby amended to clarify these distinctions.

With respect to the rejection of claim 20, the examiner has missed the main point, that content and key are routed separately. The present invention separates the content from the content key and sends them through different elements of the system that do not interact and, if implemented properly, cannot cooperate to combine the message pieces prior to their arrival at the recipient agent. This feature does not appear in Aggarwal, and therefore cannot be dismissed so readily. This claim is hereby amended to sharpen its description.

With respect to the rejection of claim 16, it is neither obvious nor non-novel that the process provides an agent while Aggarwal provides Aplic1 and Aplic2. Since those programs are transient, while the private messaging agent persists, there is a difference that remains significant. Therefore, this claim is amended to clarify this significant point.

With respect to the rejection of claim 17, the examiner has ignored the key issue that when an account is established in the present invention by a courier's foreground element, pertinent information must be distributed to the background element. Interpreting this claim in the context of the specification reveals the depth here - the communication is strictly constrained so that an operator cannot subvert the separation of foreground and background and thereby facilitate inappropriate access to message content. This claim is amended to clarify the specific data being propagated.

With respect to the rejection of claim 24, the examiner has observed that known algorithms are being used to encrypt and sign, decrypt and validate, the message as it flows through the method, just as in Aggarwal. However, the examiner has missed the forest for the trees, in that the specific order of processing is significantly different here than in any prior art. As explained in detail in the specification of application 10/701,355, the novel order of encryption and decryption provides for end to end message headers, including recipient lists, to be encrypted where in prior art messaging systems this information is clear. With the extension in the present invention to multiple couriers, the cycle of encryption and decryption is extended to accomplish this same end over the entire path of each message. The claim is amended to clarify the order of processing.

With respect to the rejection claims 25-28, the key point here is that the message handling sequence is novelly and nonobviously enhanced to handle the separation of background and foreground message parts in background and foreground courier elements. Therefore, these four claims have been combined into a single one, with claim 28 being the amended survivor and claims 25-27 being cancelled.

Thank you for the opportunity to respond to the office action.

Respectfully submitted,

James W. Bishop, Jr.

3876 Clovergate Drive

Colorado Springs, CO 80920
719-282-7767